*The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.*

**DATE(S) ISSUED:**
12/14/2011

**SUBJECT:**
Vulnerability in Microsoft Windows OLE Could Allow For Remote Code Execution (MS11-093)

**OVERVIEW:**
A remote code execution vulnerability has been discovered in Microsoft Windows Object Linking and Embedding (OLE) technology that could allow attackers to take complete control of affected systems. OLE technology is a Windows protocol that provides a platform for applications to access and manipulate functionalities that are made available by other applications. This vulnerability can be exploited by opening a rich document file format containing a specially crafted OLE object. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

**SYSTEMS AFFECTED:**
- Windows XP
- Windows Server 2003

**RISK:**
**Government**:
- Large and medium government entities: **High**
- Small government entities: **High**

**Businesses:**
- Large and medium business entities: **High**
- Small business entities: **High**

**Home users: High**

**DESCRIPTION:**
A vulnerability has been identified in Microsoft Windows Object Linking and Embedding (OLE) that could allow remote code execution. This vulnerability may be exploited if a user opens a rich document file format (e.g. .DOC, .PDF, .ODF, etc.) containing a specially crafted OLE object.

Successful exploitation of this vulnerability could result in the attacker gaining the same rights as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

**RECOMMENDATIONS:**
The following actions should be taken:

- Apply appropriate patches provided by Microsoft to vulnerable systems immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Do not open email attachments or click on URLs from unknown or untrusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails, IM (Instant Messages) or attachments especially from un-trusted sources.

**REFERENCES:**
**Microsoft:**
http://technet.microsoft.com/en-us/security/bulletin/ms11-093/
http://msdn.microsoft.com/en-us/library/ms693383

**Secunia:**
http://secunia.com/advisories/47207/

**Security Focus:**
http://www.securityfocus.com/bid/50977/

**CVE:**
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-3400